

Second Edition

AWS® Certified Security

STUDY GUIDE

SPECIALTY (SCS-C02) EXAM

**Includes one year of FREE access after activation to the
interactive online learning environment and study tools:**

2 custom practice exams

Over 100 electronic flashcards

Searchable key term glossary

**MAURICIO MUÑOZ, DARÍO GOLDFARB,
ALEXANDRE M.S.P. MORAES, OMNER BARAJAS,
ANDRÉS GONZÁLEZ SANTOS, ROGERIO KASA**

 **SYBEX®**
A Wiley Brand

AWS[®]

Certified Security Study Guide

Specialty (SCS-C02) Exam
Second Edition



AWS[®]

Certified Security Study Guide

Specialty (SCS-C02) Exam
Second Edition



Mauricio Muñoz, Darío Goldfarb,
Alexandre Matos da Silva Pires de Moraes, Omner Barajas,
Andrés González Santos, Rogerio Kasa

 **SYBEX[®]**
A Wiley Brand

Copyright © 2025 by John Wiley & Sons, Inc. All rights reserved, including rights for text and data mining and training of artificial intelligence technologies or similar technologies.

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
Published simultaneously in Canada.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise, except as permitted under Section 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 750-4470, or on the web at www.copyright.com. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at <http://www.wiley.com/go/permission>.

The manufacturer's authorized representative according to the EU General Product Safety Regulation is Wiley-VCH GmbH, Boschstr. 12, 69469 Weinheim, Germany, e-mail: Product_Safety@wiley.com.

Trademarks: Wiley and the Wiley logo are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates in the United States and other countries and may not be used without written permission. All other trademarks are the property of their respective owners. John Wiley & Sons, Inc. is not associated with any product or vendor mentioned in this book.

Limit of Liability/Disclaimer of Warranty: While the publisher and author have used their best efforts in preparing this book, they make no representations or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Neither the publisher nor author shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages. Further, readers should be aware that websites listed in this work may have changed or disappeared between when this work was written and when it is read. Neither the publisher nor authors shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

For general information on our other products and services, please contact our Customer Care Department within the United States at (800) 762-2974, outside the United States at (317) 572-3993. For product technical support, you can find answers to frequently asked questions or reach us via live chat at <https://sybexsupport.wiley.com>.

If you believe you've found a mistake in this book, please bring it to our attention by emailing our reader support team at wileysupport@wiley.com with the subject line "Possible Book Errata Submission."

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic formats. For more information about Wiley products, visit our web site at www.wiley.com.

Library of Congress Control Number: 2025911987

ISBN: 9781394253463 (paperback)
ISBN: 9781394253470 (epub)
ISBN: 9781394253487 (ePDF)

Cover Design: Wiley
Cover Image: © Jeremy Woodhouse/Getty Images

Acknowledgments

First and foremost, we offer our most profound thanks to our spouses, children, and families, whose support and understanding during our many long hours of writing and reviews gave us the time and strength to create this book. This book would not have been possible without our wonderful families.

We would also like to show our appreciation for Amazon Web Services (AWS) for providing cloud-computing platforms, APIs, and the Specialty Exam to the world at large. We are excited to be an active part of this transformative growth and development of secure cloud computing in the world today.

We'd also like to thank associate publisher Jim Minatel and acquisitions editor Ken Brown for entrusting us with the role of creating this study guide for Wiley. We also appreciate the insights of technical editor Rogerio Kasa, whose attention to detail elevated this book to the next level. Thanks also goes to managing editor Pete Gaughan, project manager Robyn Alvarez, production specialist Bala Shanmugasundaram, copy editor Kezia Endsley, and the entire team at Wiley for their guidance and assistance in making this book. We'd also like to thank all of our colleagues and experts who consulted with us while we were writing this book—too many to name here, but we are grateful for your suggestions and contributions.

And perhaps more than anyone else, we would like to thank our readers. We are grateful for the trust that you have placed in us to help you study for the exam. We wrote this book to support you in your journey.

—The Authors

About the Authors

Mauricio Muñoz is a Principal Technologist at Amazon Web Services (AWS), where he guides global customers in their journey to implement mission-critical applications into the AWS Cloud. With over 25 years of experience in information security and a CISSP certification since 2005, Mauricio has continuously expanded his expertise across various domains, including networking, application integration, analytics, and cloud computing. A passionate advocate for learning and knowledge sharing, Mauricio has served as an authorized instructor for CISSP and CEH certification training, as well as other technical certifications, including recent AWS architectural training. He is a sought-after speaker at both cloud computing and industry events, bringing valuable insights to diverse audiences. His international career spans Latin America and the United States, enriching his global perspective in technology consulting. Academically, Mauricio holds an electronics engineering degree from Pontificia Universidad Javeriana (PUJ—Colombia) and an executive MBA from Insper (Brazil), combining technical prowess with strategic business acumen.

Darío Goldfarb is a security solutions architect at Amazon Web Services in Latin America with more than 18 years of experience in cybersecurity, helping organizations from different industries improve their cyber-resiliency. Dario enjoys sharing security knowledge through speaking at public events, presenting webinars, teaching classes for universities, and writing blogs and articles for the press. He has a significant number of certifications, including CISSP, the Open Group Master IT Architect, and the AWS Security Specialty certification, and he holds a degree in systems engineering from UTN (Argentina) and a diploma in cybersecurity management from UCEMA (Argentina).

Alexandre Matos da Silva Pires de Moraes, CCIE No. 6063, worked as a systems engineer for Cisco Brazil from 1998 to 2014, in projects involving not only security and VPN technologies but also routing protocol and campus design, IP multicast routing, and MPLS networks design. He is the author of *Cisco Firewalls* (Cisco Press, 2011) and has delivered many technical sessions related to security in market events, such as Cisco Networkers and Cisco Live (Brazil, United States, United Kingdom). In 2014, Alexandre started a new journey as a director for Teltec Solutions, a Brazilian systems integrator that is highly specialized in the fields of network design, security architectures, and cloud computing. Alexandre holds the CISSP and three CCIE certifications (routing/switching, security, and service provider). He graduated with a degree in electronic engineering from the Instituto Tecnológico de Aeronáutica (ITA—Brazil) and holds a master's degree in mathematics (group theory) from Universidade de Brasília (UnB—Brazil). Alexandre also contributes, as a mathematics teacher, to preparing candidates for the national exams of military universities in Brazil, such as ITA and IME (Instituto Militar de Engenharia).

Andrés González Santos is a senior security specialist solution architect at Amazon Web Services in Latin America with more than 20 years of experience in cybersecurity. Andrés has served in various security positions, including consultant, IT architect, and security

auditor, helping organizations across diverse industries strengthen their security posture. His experience spans multiple countries, including Colombia, Ecuador, and Peru, where he has implemented strategic technological solutions for both national and international enterprises. Andrés holds a master's degree in systems engineering and a master's degree in information security. He also holds a significant number of certifications, including CISSP, CISA, CISM, CRISC, ABCP and AWS Certified Security—Specialty, AWS Networking Specialty, and AWS Certified Solutions Architect.

Omner Barajas is a security specialist solution architect at Amazon Web Services in Latin America with more than 15 years of experience in cybersecurity. During those years, Omner has taken multiple roles as security consultant, IT architect, and security auditor while helping organizations from different industries to improve their security posture. Omner has a master's degree in information security and holds a significant number of certifications, including CISSP, CISA, CISM, AWS Certified Security—Specialty, AWS Certified Solutions Architect—Professional, and PCI Internal Security Assessor (ISA).

Rogério Kasa is a Security Solutions Architect at Amazon Web Services (AWS), where he helps organizations strengthen their cloud security posture through strategic advisory and technical leadership. Since joining AWS in 2019, he has established himself as a trusted advisor in cloud security, leading the internal extended Security Community in Brazil, implementing risk-based security controls, governance frameworks, and compliance requirements. A certified professional holding CISSP/ISC2, CISM/ISACA, CCSK/CSA, and multiple AWS certifications, Rogério combines deep technical expertise with strategic insight to help organizations navigate their cloud security challenges. His work spans security automation, incident response, network security, IAM, detection/response, data protection, and the implementation of comprehensive security controls across multi-account environments.

Contents at a Glance

<i>Introduction</i>		<i>xxi</i>
<i>Assessment Test</i>		<i>xxvii</i>
Chapter 1	Security Fundamentals	1
Chapter 2	Cloud Security Principles and Frameworks	45
Chapter 3	Management and Security Governance	67
Chapter 4	Identity and Access Management	87
Chapter 5	Security Logging and Monitoring	131
Chapter 6	Infrastructure Protection	191
Chapter 7	Data Protection	293
Chapter 8	Threat Detection and Incident Response	385
Appendix A	Answers to Review Questions	431
Appendix B	Creating Your Security Journey in AWS	441
Appendix C	AWS Security Services Portfolio	449
Appendix D	DevSecOps in AWS	467
<i>Index</i>		<i>501</i>

Contents

Introduction

xxi

Assessment Test

xxvii

Chapter 1

Security Fundamentals

1

Understanding Security

2

Basic Security Concepts

6

Vulnerability, Threat, and Security Risk

6

Security Countermeasures and Enforcement

7

Confidentiality, Integrity, and Availability

7

Accountability and Nonrepudiation

7

Authentication, Authorization, and Accounting

8

Visibility and Context

8

Foundational Networking Concepts

9

The OSI Reference Model

9

The TCP/IP Protocol Stack

11

From IPv4 to IPv6

14

IPv6 Address Format and Addressing Architecture

16

Main Classes of Attacks

18

Reconnaissance

18

Password Attacks

18

Eavesdropping Attacks

19

IP Spoofing Attacks

19

Man-in-the-Middle Attacks

19

Denial-of-Service Attacks

19

Malware Attacks

20

Phishing Attacks

21

Risk Management

21

Firewalls

22

Web Proxies

23

Web Application Firewalls

23

API Discovery and Protection

23

Intrusion Detection and Intrusion Prevention

25

Protecting Email Services

26

Virtual Private Networks

27

Protecting DNS and Using Insights from DNS

27

Tools for Vulnerability Analysis and Management

28

Correlation of Security Information and Events

29

	Network Detection and Response Systems	30
	TLS/SSL Offload and Visibility	31
	Handling Security Incidents	32
	Structured Malware Protection	33
	Well-Known Security Frameworks and Models	33
	Sample Practical Models for Guiding Security Design and Operations	34
	The Security Wheel	34
	The Attack Continuum Model	35
	The Zero-Trust Model	38
	Summary	39
	Exam Essentials	39
	Review Questions	42
Chapter 2	Cloud Security Principles and Frameworks	45
	Introduction	46
	Cloud Security Principles Overview	46
	The Shared Responsibility Model	47
	Different Powers, Different Responsibilities	49
	AWS Compliance Programs	52
	AWS Artifact Portal	56
	AWS Well-Architected Framework	58
	Well-Architected Lenses	59
	Using the AWS Well-Architected Tool	60
	The AWS Marketplace	61
	Summary	62
	Exam Essentials	63
	Review Questions	64
Chapter 3	Management and Security Governance	67
	Introduction	68
	Multi-Account Management Using AWS Organizations	68
	Management Policies	70
	Authorization Policies	70
	Delegated Administration	71
	AWS Control Tower	73
	Secure and Consistent Infrastructure Deployment in AWS	75
	Infrastructure as Code Using AWS CloudFormation	75
	Tagging Strategies	77
	Sharing Resources across AWS Accounts	77
	Deploying Portfolios of Approved Services	78
	Evaluating Compliance	78
	Data Classification Using Amazon Macie	78

Evaluate Configuration Using AWS Config	79
AWS Audit Manager to Collect Compliance Evidence	80
Architecture Review and Cost Analysis	80
AWS Trusted Advisor	81
AWS Cost Explorer	81
Summary	82
Exam Essentials	83
Review Questions	85
Chapter 4	
Identity and Access Management	87
Introduction	88
IAM Overview	88
How AWS IAM Works	89
Principals	89
AWS Security Token Service	96
IAM Roles Anywhere	99
Access Management with Policies and Permissions	100
Access Management in Amazon S3	106
Policy Conflicts	109
Secure Data Transport in Amazon S3	109
Cross-Region Replication in Amazon S3	112
Amazon S3 Pre-Signed URLs	113
Identity Federation	114
Identity Use Cases	115
Amazon Cognito	115
AWS IAM Identity Center	118
Microsoft AD Federation with AWS	118
Protecting Credentials with AWS Secrets Manager	120
Secrets Permission Management	120
Automatic Secrets Rotation	120
Choosing Between AWS Secrets Manager and AWS Systems	
Manager Parameter Store	121
IAM Security Best Practices	121
Multifactor Authentication	121
Apply Least-Privilege Principle	122
Regularly Review Access to Your Environment	122
Use Conditions in IAM Policies to Further Restrict Access	122
Use IAM Roles to Provide Temporary Credentials	122
Use Federation for Your Workforce Accounts	122
Security Best Practices for Your Root User	123
Common Access Control Troubleshooting Scenarios	124
Identity Federation Problems	124

	Summary	125
	Exam Essentials	126
	Review Questions	128
Chapter 5	Security Logging and Monitoring	131
	Introduction	132
	Stage 1: Resources State	134
	AWS Config	135
	AWS Systems Manager	142
	Stage 2: Events Collection	143
	AWS CloudTrail	143
	Amazon CloudWatch Logs	157
	Amazon CloudWatch	162
	AWS Health	166
	Stage 3: Events Analysis	167
	AWS Config Rules	167
	Amazon Inspector	170
	Amazon Security Lake	172
	Amazon GuardDuty	174
	AWS Security Hub	174
	AWS Systems Manager: State Manager, Patch Manager, and Compliance	175
	AWS Trusted Advisor	177
	Stage 4: Action	178
	Summary	184
	Exam Essentials	185
	Review Questions	187
Chapter 6	Infrastructure Protection	191
	Introduction	192
	AWS Networking Constructs	192
	Network Address Translation	209
	Security Groups	215
	Network Access Control Lists	219
	Amazon VPC Transit Gateways	225
	Elastic Load Balancing	231
	VPC Endpoints	241
	VPC Flow Logs	246
	AWS Web Application Firewall	249
	AWS Shield	257
	AWS Network Firewall	259
	Amazon Inspector	263
	AWS Systems Manager Patch Manager	267

EC2 Image Builder	273
Network and Connectivity Troubleshooting Scenarios	276
VPC Network Reachability	276
Network Access Analyzer	277
VPC Security and Filtering	281
Route Tables	282
Network Gateways	282
VPC Peering	284
VPC Flow Logs	286
Summary	286
Exam Essentials	287
Review Questions	290

Chapter 7	Data Protection	293
	Introduction	294
	Symmetric Encryption	296
	Asymmetric Encryption	296
	Hash Algorithms	298
	AWS Key Management Service	300
	Managed and Data Key	303
	Customer-Managed Key and Key Hierarchy	305
	KeyID, Alias, and ARN	305
	Permissions	307
	Managing Keys in AWS KMS	312
	Creating a Key Using the Console	313
	Deleting Keys in AWS KMS	315
	Rotating Keys in KMS	316
	Understanding the Cloud Hardware Security Module	328
	Using CloudHSM with AWS KMS	333
	SSL Offload Using CloudHSM	334
	AWS Certificate Manager	335
	AWS Secret Protection Mechanisms	338
	AWS Secrets Manager	338
	AWS Systems Manager Parameter Store	341
	Protecting Your S3 Buckets	344
	Default Access Control Protection	344
	S3 Block Public Access (BPA)	344
	S3 Access Points	346
	S3 Object Lock and S3 Glacier Vault Lock	347
	Bucket and Object Encryption	350
	Amazon Macie	365
	Protecting Data on the Move in AWS	370
	Data Protection Troubleshooting Scenarios	374

	Summary	376
	Exam Essentials	377
	Review Questions	381
Chapter 8	Threat Detection and Incident Response	385
	Introduction	386
	Threat Detection	386
	Identifying Risks vs. Detecting Active Threats	387
	Automated vs. Custom Threat Detection	387
	Threat Detection Services	388
	Amazon GuardDuty	388
	AWS Security Hub	393
	AWS Trusted Advisor	397
	Amazon Detective	398
	Other Threat Detection Capabilities in AWS Services	400
	Incident Response	401
	Incident Response Life Cycle	401
	People, Technology, and Processes	403
	AWS Customer Incident Response Team	404
	Creating Your Incident Response Plan	404
	Step 1: Prepare	405
	Step 2: Implement	405
	Step 3: Monitor and Test	407
	Step 4: Update	407
	Reacting to Specific Security Incidents	408
	Abuse Notifications	408
	Insider Threat and Former Employee Access	409
	Amazon EC2 Instance Compromised by Malware	410
	Leaked Credentials	411
	Application Attacks	412
	Automating Incident Response	413
	Why Leverage Security Automations	413
	When to Automate	414
	Structure of a Security Automation	415
	How to Automate	417
	Summary	426
	Exam Essentials	426
	Review Questions	428

Appendix A	Answers to Review Questions	431
	Chapter 1: Security Fundamentals	432
	Chapter 2: Cloud Security Principles and Frameworks	433
	Chapter 3: Management and Security Governance	434
	Chapter 4: Identity and Access Management	435
	Chapter 5: Security Logging and Monitoring	436
	Chapter 6: Infrastructure Protection	437
	Chapter 7: Data Protection	438
	Chapter 8: Threat Detection and Incident Response	439
Appendix B	Creating Your Security Journey in AWS	441
	Introduction	442
	How to Prioritize Your Security Initiatives	442
	It's a Journey	443
	Security Maturity Model	444
Appendix C	AWS Security Services Portfolio	449
	Amazon Cognito	450
	Amazon Detective	451
	Amazon GuardDuty	451
	Amazon Inspector	452
	Amazon Macie	453
	Amazon Security Lake	453
	Amazon Verified Permissions	454
	AWS Artifact	455
	AWS Audit Manager	455
	AWS Certificate Manager	456
	AWS CloudHSM	456
	AWS Directory Service	457
	AWS Firewall Manager	458
	AWS Identity and Access Management	459
	AWS IAM Identity Center	459
	AWS Key Management Service	460
	AWS Network Firewall	460
	AWS Organizations	461
	AWS Payment Cryptography	462
	AWS Private Certificate Authority	462
	AWS Resource Access Manager	463
	AWS Secrets Manager	464
	AWS Security Hub	464
	AWS Shield	465
	AWS Web Application Firewall	466

Appendix D	DevSecOps in AWS	467
	Introduction	468
	Cultural Philosophies	468
	Practices	469
	Tools	471
	Dev + Sec + Ops	472
	AWS Developer Tools	473
	AWS CodeCommit	473
	AWS CodeBuild	474
	AWS CodeDeploy	475
	AWS X-Ray	475
	Amazon CloudWatch	476
	AWS CodePipeline	476
	Creating a CI/CD Using AWS Tools	477
	Creating a Repository	477
	Creating an AWS CodePipeline Pipeline	480
	Evaluating Security in Agile Development	492
	Creating the Correct Guardrails Using SAST and DAST	495
	Security as Code: Creating Guardrails and Implementing Security by Design	496
	The Top 10 Proactive Controls	496
	The 10 Most Critical Web Application Security Risks	498
<i>Index</i>		501

Table of Exercises

Exercise 2.1	Generating a PCI DSS Report in the AWS Artifact Portal	57
Exercise 2.2	Checking the ISO 27001 and ISO 27017 Reports.	58
Exercise 2.3	Using the Well-Architected Tool	61
Exercise 3.1	Viewing Compliance of Your AWS Resources.	80
Exercise 3.2	Enabling Organization View in Trusted Advisor	81
Exercise 4.1	Change the Root Account Password	90
Exercise 4.2	Enable Virtual Multifactor Authentication for the Root Account	92
Exercise 4.3	Create an IAM User with Administrator Access Permissions	93
Exercise 4.4	Create an IAM Group with Amazon S3 Read-Only Access Role	107
Exercise 4.5	Create an Amazon S3 Bucket	108
Exercise 4.6	Add a User to the AmazonS3Viewers Group	108
Exercise 4.7	Force TLS Encryption for an Amazon S3 Bucket.	110
Exercise 5.1	Set Up AWS Config	141
Exercise 5.2	Set Up a Trail in CloudTrail	155
Exercise 5.3	AWS CloudTrail Integration with Amazon CloudWatch Logs	160
Exercise 5.4	Create a Metric and an Alarm in Amazon CloudWatch	165
Exercise 5.5	AWS Config Rules	170
Exercise 5.6	AWS CloudTrail Integration with Amazon EventBridge.	182
Exercise 6.1	Create a VPC and Subnets	208
Exercise 6.2	Create an Internet Gateway	208
Exercise 6.3	Create NAT Gateways.	214
Exercise 6.4	Create Security Groups	219
Exercise 6.5	Create an NACL	225
Exercise 6.6	Create a Transit Gateway Attachment for VPC	231
Exercise 6.7	Elastic Load Balancing	240
Exercise 6.8	Work with VPC Endpoints.	246
Exercise 6.9	Check VPC Flow Logs	249
Exercise 6.10	Create and Test an AWS Web Application Firewall	256
Exercise 7.1	Create a KMS Key	313
Exercise 7.2	Create an S3 Bucket and Use a KMS Key to Protect It.	319
Exercise 7.3	Protecting RDS with KMS.	321
Exercise 7.4	Protecting EBS with KMS.	326

Exercise 7.5	Protect Your S3 Buckets with Block Public Access Settings and Service Control Policy.	357
Exercise 7.6	Replicate Encrypted S3 Objects Across Regions	360
Exercise 7.7	Protect Your S3 Buckets with a Resource Policy and VPC Endpoints.	362
Exercise 8.1	Enable Amazon GuardDuty in Your Account.	392
Exercise 8.2	Enable AWS Security Hub in Your Account.	397
Exercise 8.3	Enable Amazon Detective in Your Account	400
Exercise 8.4	Rotate AWS IAM Credentials	411
Exercise 8.5	Isolate Instances Using a TOR Anonymization Network	424

Introduction

As the pioneer and world leader of cloud computing, Amazon Web Services (AWS) has positioned security as its highest priority. Throughout its history, the cloud provider has constantly added security-specific services to its offerings as well as security features to its ever-growing portfolio. Consequently, the AWS Certified Security—Specialty certification offers a great way for IT professionals to achieve industry recognition as cloud security experts and learn how to secure AWS environments, both in concept and practice.

According to the AWS Certified Security Specialty Exam Guide, the corresponding certification attests your ability to demonstrate the following:

- An understanding of specialized data classifications and AWS data protection mechanisms
- An understanding of data-encryption methods and AWS mechanisms to implement them
- An understanding of secure Internet protocols and AWS mechanisms to implement them
- A working knowledge of AWS security services and features of services to provide a secure production environment
- Competency from two or more years of production deployment experience in using AWS security services and features
- The ability to make trade-off decisions regarding cost, security, and deployment complexity to meet a set of application requirements
- An understanding of security operations and risks

Through multiple choice and multiple response questions, you will be tested on your ability to design, operate, and troubleshoot secure AWS architectures composed of compute, storage, networking, and monitoring services. It is expected that you know how to deal with different business objectives (such as cost optimization, agility, and regulations) to determine the best solution for a described scenario.

The AWS Certified Security—Specialty exam is intended for individuals who perform a security role for three to five years with at least two years of hands-on experience securing AWS workloads.

What Does This Book Cover?

To help you prepare for the AWS Certified Security Specialty (SCS-C02) certification exam, *AWS Certified Security Study Guide Specialty (SCS-C02) Exam, Second Edition* explores the following topics:

Chapter 1: Security Fundamentals This chapter introduces you to basic security definitions and foundational networking concepts. It also explores major types of attacks,

along with the AAA architecture, security frameworks, practical models, and other solutions. In addition, it discusses the TCP/IP protocol stack.

Chapter 2: Cloud Security Principles and Frameworks This chapter discusses critical AWS Cloud security concepts such as its shared responsibility model, AWS hypervisors, AWS security certifications, the AWS Well-Architected Framework, and the AWS Marketplace. It also addresses both security *of* the cloud and security *in* the cloud. These concepts are foundational for working with AWS.

Chapter 3: Management and Security Governance This chapter discusses strategies to govern your workloads effectively using multiple AWS accounts and AWS Organizations to centrally manage security services with delegated administration and applying guardrails such as SCPs (Service Control Policies) as a technical solution to enforce policies across your organization. It also addresses how AWS Control Tower helps to consistently deploy architectures based on best practices and security guardrails to protect your workloads.

Chapter 4: Identity and Access Management This chapter explores AWS Identity and Access Management (IAM), which establishes the foundation for all resource interactions within AWS accounts. It covers authentication methods through various interfaces (AWS Console, CLI, and SDKs) and explains how to implement authorization through policies and permissions. The chapter also addresses critical security features, including multifactor authentication, identity federation, and AWS Secrets Manager, while emphasizing best practices for securing AWS environments. Key concepts include role-based access, cross-account permissions, and the principle of least privilege.

Chapter 5: Security Logging and Monitoring This chapter discusses how to gather information about the status of your resources and the events they produce through a four-stage framework: resources state, events collection, events analysis, and action. Key services include AWS Config, CloudTrail, CloudWatch, Inspector, Security Lake, Systems Manager, Trusted Advisor, and EventBridge, which work together to provide comprehensive visibility and automated responses to security events in AWS environments.

Chapter 6: Infrastructure Protection This chapter explores AWS networking concepts such as Amazon VPC, subnets, route tables, and other features that are related to network address translation (NAT gateways and NAT instances) and traffic filtering (security groups and network access control lists). It also addresses AWS Elastic Load Balancing and how security services such as AWS Web Application Firewall can provide secure access to your cloud-based applications. Finally, it discusses the AWS Shield and AWS's unique approach to mitigate distributed denial-of-service attacks.

Chapter 7: Data Protection This chapter discusses protecting data using a variety of security services and best practices, including AWS Key Management Service (KMS), the cloud hardware security module (CloudHSM), and AWS Certificate Manager. It also covers creating a customer master key (CMK) in AWS KMS, protecting Amazon S3 buckets, and how Amazon Macie can deploy machine learning to identify personal identifiable information (PII).

Chapter 8: Threat Detection and Incident Response This chapter covers AWS threat detection services (including GuardDuty, Security Hub, Trusted Advisor, and Detective) and incident response procedures, emphasizing both manual and automated approaches to handling security incidents. It covers the incident response life cycle, common security scenarios, and best practices for creating and implementing response plans while leveraging AWS services and automation capabilities to detect and remediate security issues effectively.

Appendix A: Answers to Review Questions This appendix provides the answers to the review questions that appear at the end of each chapter throughout the book.

Appendix B: Creating Your Security Journey in AWS This appendix discusses how to create your strategy to improve your security posture, consistently prioritizing the most important initiatives that can provide you security benefits, such as mitigating critical risks as soon as possible, thus optimizing your team's results.

Appendix C: AWS Security Services Portfolio This appendix provides an overview of the 24 AWS cloud services dedicated to security, identity, and compliance.

Appendix D: DevSecOps in AWS This appendix introduces DevSecOps, the AWS family of services that implement DevOps practices, and how security controls can be implemented in an automated pipeline.

How to Contact the Publisher

If you believe you've found a mistake in this book, please bring it to our attention. At John Wiley & Sons, we understand how important it is to provide our customers with accurate content, but even with our best efforts, an error may occur.

In order to submit your possible errata, please email it to our Customer Service Team at wileysupport@wiley.com with the subject line "Possible Book Errata Submission."

Interactive Online Learning Environment and Test Bank

Studying the material in the *AWS Certified Security Study Guide: Specialty (SCS-C02) Exam* is an important part of preparing for the AWS Certified Security Specialty (SCS-C02) certification exam, but we provide additional tools to help you prepare. The online test bank will help you understand the types of questions that will appear on the certification exam. The online test bank runs on multiple devices.

Sample Tests: The sample tests in the test bank include all the questions at the end of each chapter as well as the questions from the assessment test. In addition, there are two practice

exams with 50 questions each. You can use these tests to evaluate your understanding and identify areas that may require additional study.

Flashcards: The flashcards in the test bank will push the limits of what you should know for the certification exam. There are 100 questions provided in digital format. Each flashcard has one question and one correct answer.

Glossary: The online glossary is a searchable list of key terms introduced in this exam guide that you should know for the AWS Certified Security Specialty (SCS-C02) certification exam.

Go to www.wiley.com/go/sybextestprep to register and gain access to this interactive online learning environment and test bank with study tools. To start using these tools to study for the AWS Certified Security Specialty (SCS-C02) exam, go to www.wiley.com/go/sybextestprep to register your book and receive your unique PIN. Once you have the PIN, return to www.wiley.com/go/sybextestprep, find your book, and click register or login and follow the link to register a new account or add this book to an existing account.

AWS Certified Security Study Guide—Specialty (SCS-C02) Exam Objectives

This table shows the extent, by percentage, of each domain represented on the actual examination.

Domain	Percent of Examination
Domain 1: Threat Detection and Incident Response	14%
Domain 2: Security Logging and Monitoring	18%
Domain 3: Infrastructure Security	20%
Domain 4: Identity and Access Management	16%
Domain 5: Data Protection	18%
Domain 6: Management and Security Governance	14%
Total	100%



Exam objectives are subject to change at any time without prior notice and at AWS's sole discretion. Visit the AWS Certified Security–Specialty website (aws.amazon.com/certification/certified-security-specialty) for the most current listing of exam objectives.

Objective Map

Objective	Chapters
Domain 1: Threat Detection and Incident Response	
1.1: Design and implement an incident response plan.	2,8
1.2: Detect security threats and anomalies by using AWS services.	1,5,8
1.3: Respond to compromised resources and workloads.	8
Domain 2: Security Logging and Monitoring	
2.1: Design and implement monitoring and alerting to address security events.	1,5
2.2: Troubleshoot security monitoring and alerting.	5
2.3: Design and implement a logging solution.	5
2.4: Troubleshoot logging solutions.	5
2.5: Design a log analysis solution.	5
Domain 3: Infrastructure Security	
3.1: Design and implement security controls for edge services.	1,6
3.2: Design and implement network security controls.	1,6
3.3: Design and implement security controls for compute workloads.	6
3.4: Troubleshoot network security.	2,6
Domain 4: Identity and Access Management	
4.1: Design, implement, and troubleshoot authentication for AWS resources.	1,4
4.2: Design, implement, and troubleshoot authorization for AWS resources.	4
Domain 5: Data Protection	
5.1: Design and implement controls that provide confidentiality and integrity for data in transit.	7
5.2: Design and implement controls that provide confidentiality and integrity for data at rest.	7

Objective	Chapters
5.3: Design and implement controls to manage the life cycle of data at rest.	1,7
5.4: Design and implement controls to protect credentials, secrets, and cryptographic key materials.	7
Domain 6: Management and Security Governance	
6.1: Develop a strategy to centrally deploy and manage AWS accounts.	3
6.2: Implement a secure and consistent deployment strategy for cloud resources.	3
6.3: Evaluate the compliance of AWS resources.	3,5
6.4: Identify security gaps through architectural reviews and cost analysis.	3

Assessment Test

1. Which one of the following components should not influence an organization's security policy?
 - A. Business objectives
 - B. Regulatory requirements
 - C. Risk
 - D. Cost-benefit analysis
 - E. Current firewall limitations
2. Consider the following statements about the AAA architecture:
 - I. Authentication deals with the question "Who is the user?"
 - II. Authorization addresses the question "What is the user allowed to do?"
 - III. Accountability answers the question "What did the user do?"Which of the following is correct?
 - A. Only I is correct.
 - B. Only II is correct.
 - C. I, II, and III are correct.
 - D. I and II are correct.
 - E. II and III are correct.
3. What is the difference between denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks?
 - A. DDoS attacks have many targets, whereas DoS attacks have only one each.
 - B. DDoS attacks target multiple networks, whereas DoS attacks target a single network.
 - C. DDoS attacks have many sources, whereas DoS attacks have only one each.
 - D. DDoS attacks target multiple layers of the OSI model and DoS attacks only one.
 - E. DDoS attacks are synonymous with DoS attacks.
4. Which of the following options is incorrect?
 - A. A firewall is a security system aimed at isolating specific areas of the network and delimiting domains of trust.
 - B. Generally speaking, the web application firewall (WAF) is a specialized security element that acts as a full-reverse proxy, protecting applications that are accessed through HTTP.
 - C. Whereas intrusion prevention system (IPS) devices handle only copies of the packets and are mainly concerned with monitoring and alerting tasks, intrusion detection system (IDS) solutions are deployed inline in the traffic flow and have the inherent design goal of avoiding actual damage to systems.

- D. Security information and event management (SIEM) solutions are designed to collect security-related logs as well as flow information generated by systems (at the host or the application level), networking devices, and dedicated defense elements such as firewalls, IPSs, IDSs, and antivirus software.
5. In the standard shared responsibility model, AWS is responsible for which of the following options?
 - A. Regions, availability zones, and data encryption
 - B. Hardware, firewall configuration, and hypervisor software
 - C. Hypervisor software, regions, and availability zones
 - D. Network traffic protection and identity and access management
 6. Which AWS service allows you to generate compliance reports that enable you to evaluate the AWS security controls and posture?
 - A. AWS Artifact
 - B. AWS Trusted Advisor
 - C. AWS Well-Architected Tool
 - D. Amazon Inspector
 7. Which of the following contains a definition that is not a pillar from the AWS Well-Architected Framework?
 - A. Security and operational excellence
 - B. Reliability and performance efficiency
 - C. Cost optimization and availability
 - D. Security and performance efficiency
 8. Which of the following services provides a set of APIs that controls access to your resources on the AWS Cloud?
 - A. AWS AAA
 - B. AWS IAM
 - C. AWS Authenticator
 - D. AWS AD
 9. Regarding AWS IAM principals, which option is *not* correct?
 - A. A principal is an IAM entity that has permission to interact with resources in the AWS Cloud.
 - B. They can only be permanent.
 - C. They can represent a human user, a resource, or an application.
 - D. They have three types: root users, IAM users, and roles.